

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА №18  
ИМЕНИ ВИТАЛИЯ ЯКОВЛЕВИЧА АЛЕКСЕЕВА**

**П Р И К А З**

г. Сургут

26.10.2022

№ Ш18-13-826/2

Об организации и проведении мероприятий по информационной безопасности при работе в сети «Интернет» с утвержденным перечнем мероприятий по информационной безопасности при работе в сети «Интернет»

В соответствии с законами Российской Федерации от 24.07.1998 № 124 «Об основных гарантиях прав ребенка в Российской Федерации», от 25.07.2002 № 114 «О противодействии экстремистской деятельности», от 27.07.2006 № 149 «Об информации, информационных технологиях и о защите информации», от 29.12.2010 № 436 «О защите детей от информации, причиняющей вред их здоровью и развитию», от 28.07.2012 №139 «О защите детей от информации, причиняющей вред их здоровью и развитию», концепцией информационной безопасности детей, утвержденной распоряжением Правительства Российской Федерации от 02.12.2015 № 2471-р, методическими рекомендациями по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, также не соответствующей задачам образования, приказом Департамента образования и молодежной политики ХМАО - Югры от 19.08.2013 № 798 «О контроле за Интернет-ресурсами, используемыми в деятельности образовательными учреждениями», приказа департамента образования Администрации города от 26.08.2019 312-05-645/9 «Об обеспечении информационной безопасности при работе в сети интернет», в целях исполнения законодательства в области информационной безопасности

**ПРИКАЗЫВАЮ:**

1. Утвердить:

1.1. Положение об организации и обеспечении информационной безопасности обучающихся при работе в сети «Интернет» в МБОУ СОШ №18 имени В.Я. Алексева, согласно приложению 1.

1.2. План мероприятий по обеспечению информационной безопасности обучающихся при работе в сети «Интернет» на 2022-2023 учебный год, согласно приложению 2.

2. Назначить ответственными:

2.1. За организацию и обеспечение информационной безопасности на 2022-2023 учебный год заместителя директора заместителя директора по учебно-воспитательной работе Исмайлову И.В.

2.2. За организацию антивирусной защиты и технического обеспечения контентной фильтрации технического специалиста Галингера А.И.

2.3. Ознакомить сотрудников с Положением об организации и обеспечении информационной безопасности обучающихся при работе в сети «Интернет» в трехдневный срок с момента издания настоящего приказа.

3. Педагогическому составу:

3.1. Осуществлять контроль за использованием учащимися ресурсов сети Интернет в урочное и внеурочное время.

4. Контроль за выполнением приказа возложить на заместителя директора по учебно-воспитательной работе Исмайлову И.В.

Директор

**Подписано электронной подписью**

Сертификат:  
00BB334ED0A2ACA3F3374EC2F2E60A31DC  
Владелец:  
Калганова Елена Валериевна  
Действителен: 04.04.2022 с по 25.06.2023

Е.В. Калганова

С приказом ознакомлена:  
И.В. Исмайлова  
А.И. Галингер

Положение  
об организации и обеспечении информационной безопасности  
обучающихся при работе в сети «Интернет»  
в МБОУ СОШ №18 имени Виталия Яковлевича Алексева

1. Общие положения

1.1. Настоящее Положение разработано на основании следующих документов:

1.1.1. «Конвенция о правах ребенка» (одобрена Генеральной Ассамблеей ООН 20.11.1989) (вступила в силу для СССР 15.09.1990);

1.1.2. Федеральный закон от 24.07.1998 №124 «Об основных гарантиях прав ребенка в Российской Федерации»;

1.1.3. Федеральный закон от 25.07.2002 №114 «О противодействии экстремисткой деятельности»;

1.1.4. Федеральный закон от 27.07.2006 №149 «Об информации, информационных технологиях и о защите информации»;

1.1.5. Федеральный закон от 29.12.2010 №436 «О защите детей от информации, причиняющей вред их здоровью и развитию» и все его изменения;

1.1.6. Федеральный закон от 28.07.2012 №139 «О защите детей от информации, причиняющей вред их здоровью и развитию»;

1.1.7. Концепция информационной безопасности детей, утвержденная распоряжением Правительства Российской Федерации от 02.12.2015 № 2471-р;

1.1.8. Методические рекомендации Совета Федерации Федерального собрания Российской Федерации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;

1.1.9. Приказ Департамента образования и молодежной политики ХМАО - Югры от 19.08.2013 №798 «О контроле за Интернет-ресурсами, используемыми в деятельности образовательными учреждениями».

1.2. Настоящее положение разработано с целью ограничения доступа в МБОУ СОШ №18 имени Виталия Яковлевича Алексева (далее – ОО) к информации, причиняющей вред здоровью и (или) развитию обучающихся, а также не соответствующей целям и задачам образования.

1.3. Контроль организации контентной фильтрации (далее – КФ) ресурсов сети «Интернет» в ОО осуществляется департаментом образования и муниципальным автономным учреждением «Информационно-методический центр» (далее – МАУ «ИМЦ»).

1.4. Все обязанности по обеспечению эффективного функционирования средств контентной фильтрации (далее – СКФ) регулируются локальными нормативными актами образовательной организации (приказами, положением и должностными инструкциями, утвержденными директором образовательной организации).

1.5. Ознакомление с положением и его соблюдение обязательно для всех сотрудников образовательной организации.

1.6. Срок действия данного Положения не ограничен. Положение действует до принятия нового.

2. Обязанности директора и сотрудников школы по обеспечению информационной безопасности обучающихся при работе в сети «Интернет»

2.1. Директор школы:

2.1.1. осуществляет общее управление по организации КФ в образовательной организации;

2.1.2. устанавливает правила по ограничению физического доступа обучающихся к автоматизированным рабочим местам (далее - АРМ) педагогов и сотрудников образовательной организации (например: запретить нахождение обучающихся в кабинетах на перемене в отсутствие сотрудника образовательной организации, где есть АРМ с выходом в сеть «Интернет»);

2.1.3. назначает заместителя директора, ответственного за организацию и обеспечение информационной безопасности в образовательной организации;

2.1.4. назначает специалиста, ответственного за техническое сопровождение СКФ ресурсов сети «Интернет»;

2.1.5. принимает решение о создании совета по обеспечению информационной безопасности обучающихся (далее - Совет) и утверждает его состав;

2.1.6. разрабатывает план мероприятий образовательной организации по обеспечению информационной безопасности обучающихся при работе в сети «Интернет»;

2.1.7. несет полную ответственность за качественное выполнение Плана мероприятий.

2.2. Ответственный заместитель директора образовательной организации:

2.2.1. исполняет План мероприятий;

2.2.2. контролирует деятельность сотрудников образовательной организации, в том числе технического специалиста по исполнению Плана мероприятий;

2.2.3. принимает решение о разрешении/блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети «Интернет»;

2.2.4. осуществляет хранение в сейфе логинов и паролей, установленных на операционную систему и программу, осуществляющую КФ на персональных компьютерах обучающихся, и предоставляет их сотрудникам МАУ «ИМЦ» для выполнения функциональных обязанностей.

2.3. Технический специалист:

2.3.1. исполняет План мероприятий;

2.3.2. принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательной деятельности.

2.4. Совет по обеспечению информационной безопасности обучающихся (при его наличии):

2.4.1. принимает участие в реализации Плана мероприятий.

2.5. Сотрудники образовательной организации:

2.5.1. соблюдают в своей профессиональной деятельности законодательство РФ в области информационной безопасности, в том числе КФ при работе с обучающимися в сети «Интернет»;

2.5.2. исполняют План мероприятий;

2.5.3. принимают меры по пресечению обращений, обучающихся к ресурсам, не имеющим отношения к образовательной деятельности;

2.6. Сотрудникам образовательной организации разрешается отключать СКФ на своих персональных устройствах или устройствах, предоставленных педагогическому работнику, только после осуществления образовательной деятельности и отсутствия обучающихся на территории образовательной организации, а также получения письменного согласия от директора или заместителя директора образовательной организации с указанием или пояснением целей отключения СКФ и временных сроках отключения СКФ с занесением информации в журнал работы КФ.

2.7. Сотрудникам образовательной организации запрещается:

2.7.1. При работе на автоматизированном рабочем месте:

2.7.1.1. работать в сети «Интернет», без прохождения соответствующего инструктажа;

2.7.1.2. подключать оборудование, проводить настройку сети и СКФ самостоятельно (кроме технического специалиста, отвечающего за техническое сопровождение СКФ ресурсов сети «Интернет»);

2.7.1.3. отключать СКФ во время нахождения на территории образовательной организации обучающихся;

2.7.1.4. использовать поисковые системы Yandex, Google, Rambler, Mail.ru и т.д., кроме поисковых систем сервиса ООО «СкайдНС», <http://search.skydns.ru>;

2.7.1.5. обращаться к ресурсам, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают законодательство Российской Федерации (эротика, порнография, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности);

2.7.1.6. осуществлять любые сделки через сеть «Интернет»;

2.7.1.7. загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;

2.7.1.8. распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы;

2.7.1.9. загружать и распространять:

2.7.1.9.1. материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо - ограничения функциональности компьютерного или телекоммуникационного оборудования;

2.7.1.9.2. программы, для осуществления несанкционированного доступа, серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети «Интернет», а также размещать ссылки на вышеуказанную информацию.

2.7.10. Пользоваться чужими учетными данными при использовании сетевых сервисов, предполагающих авторизацию.

2.7.11. Работать на своих персональных (личных) устройствах без СКФ в присутствии обучающихся на территории образовательной организации.

**План мероприятий по обеспечению информационной безопасности обучающихся при работе в сети «Интернет»  
на 2022-2023 учебный год**

№	Мероприятие	Сроки	Сроки предоставления отчетов в МАУ «ИМЦ»
<b>І. Деятельность руководителя образовательной организации, заместителя руководителя образовательной организации</b>			
1.	Издание приказа «О создании совета по обеспечению информационной безопасности обучающихся», утверждение состава совета, положения о совете. Организация работы совета по обеспечению информационной безопасности обучающихся	Сентябрь - октябрь	
2.	Изучение нормативных правовых документов, методических рекомендаций и издание (актуализация) организационно-распорядительных документов образовательной организации по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети «Интернет»	Сентябрь – октябрь	
3.	Ознакомление работников образовательной организации с методическими рекомендациями по ограничению доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, локальными нормативными актами по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети «Интернет»	Сентябрь – октябрь	
4.	Ознакомление работников образовательной организации с сайтами в сети «Интернет», включенными в Реестр безопасных образовательных сайтов	Сентябрь-октябрь	-
5.	Информирование работников образовательной организации, обучающихся и их родителей (законных представителей) об ответственности за нарушение требований законодательства Российской Федерации и организационно-распорядительных документов образовательной организации по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети «Интернет»	Сентябрь-октябрь	

6.	Инструктаж педагогических работников по ограничению доступа к информации, причиняющей вред здоровью и (или) развитию обучающихся, а также не соответствующей задачам образования, в ходе образовательной деятельности. Ведение журнала инструктажа педагогических работников	2 раза в год	В течение 3 рабочих дней с даты проведения мероприятия
7.	Контроль качества работы систем контентной фильтрации в образовательной организации	Раз в квартал	-
8.	Организация преподавания обучающимся основ информационной безопасности в рамках реализации образовательной программы (в соответствии с методическими рекомендациями по основам информационной безопасности для обучающихся общеобразовательных организаций с учётом информационных, потребительских, технических и коммуникативных аспектов информационной безопасности)	В течение учебного года	В течение 3 рабочих дней с даты проведения мероприятия
<b>II. Деятельность технического специалиста</b>			
11.	Настройка (установка) технических средств, применяемых при организации доступа к сети «Интернет» (компьютерное оборудование, сетевое оборудование, системное и прикладное программное обеспечение) (в соответствии с инструкциями по настройке средств контентной фильтрации в образовательной организации)	Август	
12.	Установка, конфигурация, настройка режимов работы технических средств контентной фильтрации	Август	-
13.	Проверка работоспособности средств контентной фильтрации (в соответствии с инструкцией по проверке работоспособности средств контентной фильтрации в образовательной организации)	Не менее 3 раз в течение учебного года	
14.	Настройка ограничения доступа обучающихся к автоматизированному рабочему месту педагогов путем установки логина и пароля на операционную систему Настройка выхода в ждущий режим по истечении 5 минут неактивности	Август	
15.	Ведение документации образовательной организации в области информационной безопасности обучающихся - акт установки контентной фильтрации в образовательной организации	В течение учебного года	

	(акт установки криптошлюза Ростелеком); - журнал контроля контентной фильтрации; - журнал обнаружения образовательной организацией сайтов, заблокированных ошибочно, которые необходимо разблокировать для педагогов журнал регистрации случаев обнаружения образовательной организацией сайтов, причиняющих вред здоровью и развитию обучающихся		
16.	Составление докладной записки на имя директора образовательной организации по каждому выявленному факту доступа к ресурсам, не имеющим отношения к образовательной деятельности	В течение учебного года	В течение 3 дней
17.	Передача информации о ресурсах сети «Интернет», предоставленной сотрудниками образовательной организации, представителями Совета и администрацией школы, в Минцифры для добавления в список запрещенных сайтов, передача информация об учебных сайтах, которые недоступны для учителей.	В течение учебного года	-
18.	Обеспечение возможности использования обучающимися и сотрудниками образовательной организации дополнительных разрешенных ресурсов сети «Интернет» в компьютерных классах (кабинетах информатики) и библиотеке в урочное и внеурочное время по заявке сотрудника образовательной организации	В течение учебного года	
19.	Предоставление доступа к персональным компьютерам обучающихся сотрудникам МАУ «ИМЦ» через программу удаленного доступа (Lite Manager, Ammyu Admin, Anydesl) и непосредственно к рабочим местам обучающихся в любое время в течение рабочего времени	В течение учебного года	
20.	Размещение на официальном сайте образовательной организации (Раздел «Информационная безопасность») информации по вопросам обеспечения информационной безопасности детей (в соответствии с письмом Минобрнауки России от 14.03.2018 N 08-1184 «О направлении информации»)	В течение учебного года	
<b>III. Деятельность Совета по обеспечению информационной безопасности обучающихся</b>			



21.	Участвует в мероприятиях образовательной организации по информационной безопасности	В течение учебного года	
22.	Осуществляет мониторинг качества работы системы контентной фильтрации Предоставляет результат мониторинга качества работы СКФ директору	Ежеквартально	
<b>IV. Деятельность сотрудников образовательной организации</b>			
23.	Прохождение педагогическими и иными работниками образовательной организации программы повышения квалификации на сайте Единыйурок.рф по направлению «Безопасное использование сайтов в сети «Интернет» в образовательном процессе в целях обучения и воспитания обучающихся в образовательной организации»	Раз в два календарных года	В течение 3 рабочих дней с даты проведения мероприятия
24.	Участие сотрудников образовательной организации в работе Экспертного совета по информатизации системы образования и воспитания при Временной комиссии Совета Федерации по развитию информационного общества в сфере образования и воспитания	В течение учебного года	
25.	Информирование родителей (законных представителей) обучающихся о существующих угрозах в сети «Интернет», о методах и способах защиты детей от информации, причиняющей вред здоровью и (или) развитию детей	Сентябрь-октябрь	В течение 3 рабочих дней с даты проведения мероприятия
26.	Инструктаж обучающихся о правилах использования сети «Интернет» Ведение журнала инструктажа обучающихся	Не менее 2 раз в учебном году	
27.	Контроль использования обучающимися ресурсов сети «Интернет» в урочное и внеурочное время в ОО	В течение учебного года	
28.	Информирование технического специалиста о фактах нарушения обучающимися установленных правил пользования сети «Интернет»	В течение учебного года	
29.	Организация просветительской работы с обучающимися и их родителями (законными представителями) по повышению культуры информационной безопасности	В течение учебного года	
30.	Организация и проведение мероприятия воспитательного характера в рамках дня солидарности борьбы с терроризмом по теме «Порядок действия при обнаружении в сети «Интернет» контента террористического содержания	3 сентября	

	либо сведений о подготавливаемых к совершению в образовательных учреждениях насильственных преступлениях»		
31.	Организация участия обучающихся, родителей (законных представителей) обучающихся образовательной организации в деятельности Межрегионального детского движения в области обеспечения безопасности и развития детей в информационном пространстве «Страна молодых»	В течение учебного года	В течение 3 рабочих дней с даты проведения мероприятия
32.	Проведение Единого урока по безопасности в сети «Интернет»	Октябрь	
33.	Проведение серии мероприятий проекта «Сетевичок» для обучающихся	Октябрь- ноябрь	
34.	Проведение Всероссийской контрольной работы по информационной безопасности на сайте <a href="http://www.Единыйурок.дети">www.Единыйурок.дети</a>	Октябрь-ноябрь	
35.	Использование в работе образовательных программ, направленных на формирование у обучающихся навыков безопасного поведения в информационной среде, рекомендованных Экспертным советом по информатизации системы образования и воспитания при Временной комиссии Совета Федерации по развитию информационного общества	В течение учебного года	